

Cibercontrol Social



Conoce y evita las formas
con las que espían
nuestra vida en la Red

BIG BROTHER



**IS WATCHING
YOU**

¿Qué temas trataremos?

- **Sistemas actuales de control social por Internet**
 - Echelon
 - Carnivore
 - El peligro de sistemas Single-Sign-On: Microsoft Passport.Net
- **Trojanos en nuestros PCs**
 - Magic Lantern y derivados
 - Activación por Internet
- **Medidas hardware para el cibercontrol social**
 - TC, ¿confiable para quien?
 - Localización geográfica sin GPS vía GSM
 - Tecnología RFID
- **¡Ni un paso atrás! Hacktivismo**
 - Contra-ataque: Netstrike!!!
 - Hacklabs, Hack in the streets, Hackmeetings
- **Conclusiones**

Sistemas actuales de control social por Internet

- **Echelon**
 - Sistema de espionaje al ciudadano de a pie en su vida cotidiana, todo el mundo es un enemigo potencial.
 - No sólo las comunicaciones personales por Internet son filtradas y espiadas, sino muchas conversaciones telefónicas, móviles, fax y GPS.
 - Funcionaba con un sistema de "palabras clave" que activan el filtrado (Ejemplo: "he bombed!").
 - Participan Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda.
 - El Parlamento Europeo hizo pública su existencia en mayo de 2001.

Sistemas actuales de control social por Internet

- **Echelon**
 - **Técnicamente le lleva 10 años de ventaja a Internet:**
 - **Cuando ARPANet se abrió al público, la red "Platform" que sustenta Echelon ya era mucho más potente (sistemas de satélites y cables submarinos).**
 - **Echelon descartó ya en los 80 el sistema de palabras clave que utiliza actualmente Google (¡¡en los 80 yo grababa mis juegos de Spectrum de la radio!!).**
 - **Actualmente ha solicitado la patente para un método de búsqueda basado en campos semánticos, por lo que ya será obsoleto y estarán utilizando otro.**
 - **Han hecho lo mismo con un sistema de reconocimiento de voz automatizado global.**

Sistemas actuales de control social por Internet

- **Echelon**
 - **Margaret Newsham: "Ya en 1979 podíamos rastrear a una persona determinada y captar su conversación telefónica en tiempo real".**
 - **En 1984, los satélites de inteligencia norteamericanos "lograron fotografiar un sello de correos en el suelo, por lo que es casi imposible imaginar la versatilidad de los sistemas de hoy".**
 - **"Con la tecnología actual, toda comunicación electrónica es un objetivo para los servicios de inteligencia: tus transferencias de dinero, tus operaciones de Bolsa, tus conversaciones políticas y tu comunicación privada. Todo es puesto al descubierto".**

Sistemas actuales de control social por Internet

- **Carnivore**

- Sistema de espionaje creado por la NSA, Agencia de Seguridad Nacional de Estados Unidos, y el FBI.
- Colaboración con empresas como Microsoft o Cisco, líderes en el mercado del software y el hardware de equipamientos de red respectivamente.

- **En palabras del propio FBI:**

"Carnivore es un sistema computacional diseñado para permitir al FBI; en colaboración con un proveedor de Internet (ISP) se haga valer una orden judicial que exige la recolección de cierta información en relación al correo electrónico u otros tipos de comunicaciones electrónicas de un usuario específico que es objeto de investigación".

- **Bastante similar a la nueva Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE)**

Sistemas actuales de control social por Internet

- **Sistemas "Single-Sign-On", Microsoft Passport.Net**
 - Amenaza contra la intimidad de los "netizens".
 - Mediante Passport.Net es posible introducir un usuario y contraseña en uno de los sitios en los que se utilice y no tener que volver a enseñar ese "pasaporte virtual" en el resto de sitios que funcionan con este sistema.
(Ejemplo: Hotmail -> Ebay).
- **Problema: correlaciones y data-mining**
 - **Ejemplo:**
 - Comprar medias: ¿regalo a tu hermana?
 - Comprar rifle de caza: ¿tienes un coto de caza?
 - Comprar sierra de metal: ¿bricomania?
 - Suma de todas: ¿atraco a un banco?

Troyanos en nuestros PCs

- **"Magic Lantern"**
 - **Desarrollado por el FBI y la CIA.**
 - **Con el beneplácito de los dos grandes pesos pesados de Internet: Microsoft y CISCO.**
 - **Con la colaboración de "hackers" como el grupo "Cult of the Dead Cow", famoso por el troyano "Back Oriffice".**
 - **Las empresas de antivirus se mantienen en una extraña ambigüedad: ¿detectan el troyano? ¿fidelidad al cliente o al Gobierno de USA? Microsoft y CISCO ya han decidido.**

Trojanos en nuestros PCs

- **Sistemas de activación por Internet:**
 - Antiguamente se utilizaban números de serie, "mochilas", etc. para activar los programas.
 - Todo eso está olvidado, activación por Internet.
 - ¿Cuánta información personal revelan tus programas al conectarse con la empresa que los creó?
- **Muchos posibles objetivos:**
 - Marketing, combatir la piratería, espionaje industrial.
- **Windows XP se conecta de 20 formas diferentes y espía software de terceros (tecDUMP).**

Medidas hardware de cibercontrol

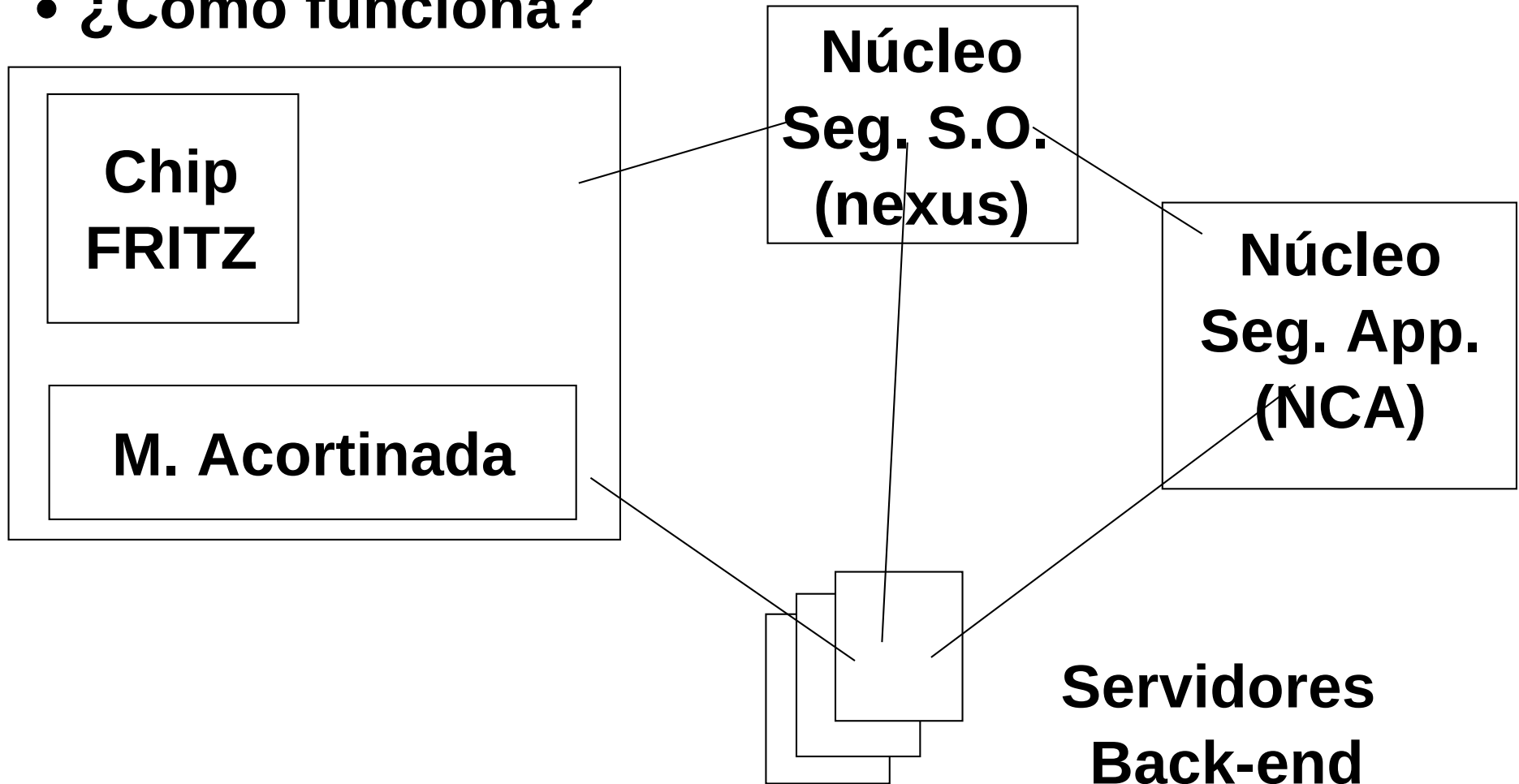
- **TC / TCG / TCPA / LaGrande / Palladium**
 - **El Grupo para la Informática Fiable es una alianza entre Microsoft, Intel, IBM, HP y AMD.**
 - **Conseguir un ordenador "más seguro"...**
 - ¿Para quién?
 - **Más seguro para las empresas de software y contenidos audiovisuales (Microsoft, Disney).**
 - **Más inseguro para su propietario -> Stallman lo califica de Informática Traidora.**
 - **Su aplicación inicial era el Control de Derechos Digitales (DRM): venderte un DVD que sólo funciona en 1 PC y el día de tu cumpleaños.**

Medidas hardware de cibercontrol

- **TC / TCG / TCPA / LaGrande / Palladium**
 - **TC también hará mucho más difícil ejecutar software sin licencia -> ¡Bill Gates lleva años intentando que los chinos paguen por el software que usan!**
 - **¿Es esto tan malo? Bueno...**
 - **La mayoría del Software Libre será tratado como software sin licencia y no funcionará.**
 - **Nuestros documentos dejan de ser nuestros, están protegidos digitalmente y pueden ser borrados remotamente -> Censura remota, "Traitor tracing", pérdida de pruebas...**

Medidas hardware de cibercontrol

- TC / TCG / TCPA / LaGrande / Palladium
 - ¿Cómo funciona?



Medidas hardware de cibercontrol

- **TC / TCG / TCPA / LaGrande / Palladium**
 - **¿Pero todo esto no se puede hackear?**
 - **En una primera fase se podría "escuchar" digitalmente el flujo de datos entre el procesador y el chip Fritz.**
 - **Cuando el chip Fritz se integre dentro del procesador esto será inviable.**
 - **¡Pues nos negamos a usarlo!**
 - **Quizá tu proveedor de Internet te obligue a conectarte desde un ordenador "seguro".**
 - **Quizá tu banco te obligue a lo mismo.**
- ¡¡¡PROTESTAR, PROTESTAR y PROTESTAR!!!**

Medidas hardware de cibercontrol

- **TC / TCG / TCPA / LaGrande / Palladium**
 - **¿Cuándo llegará todo esto?**
 - **ATMEL ya está vendiendo un chip Fritz.**
 - **Puedes comprarlo de serie en un IBM Thinkpad.**
 - **Algunas de estas maravillosas características ya están implementadas en WindowsXP y la X-Box.**
 - **El Enterprise Rights Management ya se incluye con todos los Windows 2003 Server.**
- **Guardad vuestros viejos PCs en el desván, nos harán falta cuando las cosas se pongan duras ;-)**

Medidas hardware de cibercontrol

- **Localización geográfica por telefonía móvil**
 - Desde el principio de la telefonía móvil se ha podido rastrear geográficamente un teléfono conectado a la red. Es ilegal, pero hasta la máquina de cafés de la NSA es ilegal :-D
 - Se basa en que las antenas de GSM están sectorizadas (120° cada sector) y en los tiempos de retardo:
 - Cuantas más densidad de antenas haya, mayor precisión.
 - ¿Un hacker podría mentir en los tiempos de retardo? Tampoco consigue ser invisible.

Medidas hardware de cibercontrol

- **Localización geográfica por telefonía móvil**
 - Actualmente se ofrece comercialmente en España por el RACC o servicios como "¿Dónde?" de Amena:
 - Seguimiento sólo a móviles que hayan dado su "consentimiento": flota de camiones, adolescentes...
 - Coste mínimo, SMSs.
- Vuestros móviles son como la bola roja que se saca Schwarzenegger en Desafío Total por la nariz (yo no tengo móvil ;-)).

Medidas hardware de cibercontrol

- **RFID (Radio Frequency IDentification)**
 - En la misma línea que la localización anterior, pero de forma pasiva.
 - Los productos comerciales pasarán de tener código de barras a tener circuitos RFID.



Medidas hardware de cibercontrol

- **RFID (Radio Frequency IDentification)**
 - **Son pasivos, no necesitan energía, "rebotan" la señal emitida por una antena, localizando al "objetivo".**
 - **En principio podrían valer para hacer inventarios automáticos, detectar pequeños robos (los de Yo-mango las conocen bien), etc.**
 - **En la práctica sirven para cibercontrolar: se han implantado en colegios privados de USA: ya no hace falta pasar lista, controlar a los niños en cada momento, ¡es genial!**

Medidas hardware de cibercontrol

- **RFID (Radio Frequency IDentification)**
 - **¿Es esto otra de tus paranoias?**
 - **Sí, claro, pero ya están aquí...**
 - **Gillete comercializa maquinillas con RFID para controlar el hábito de sus consumidores... ¿lo sabíais?**
 - **Wall-Mart, la cadena de supermercados más grande de USA lo comenzará a obligar a sus proveedores dentro de 3 años.**
- **Los circuitos RFID caben hasta en una lentilla, desconfiad hasta de las pegatinas de los plátanos.**

Medidas hardware de cibercontrol

- **RFID (Radio Frequency IDentification)**



¡Ni un paso atrás! Hacktivismo

- **El hacktivismo...**
 - **¿suma de hacking + activismo?**
 - **comenzó siendo despreciado por los hackers y activistas:**
 - **hackers: "sois tecnológicamente patéticos, peores que los 'script kiddies' ".**
 - **activistas: "usais la tecnología, un instrumento del poder".**
 - **ha realizado diferentes campañas en la red, sin eficiencia práctica pero con mucha eficiencia mediática.**

Contraataque: Netstrike!!!

- **Frente al control existen varias reacciones:**
 - **Iniciativas y campañas:**
 - Campañas contra la aprobación de las patentes de software.
 - Campañas de sensibilización acerca del Software Libre, la privacidad en Internet, etc.
 - Portales de (contra)información (normalmente basados en "open publishing").
 - **Hacktivismo:**
 - Netstrikes: Ataques por saturación (DoS: Denial of Service) a sistemas gubernamentales normalmente.
 - Acciones tipo www.hactivist.com.

Hacklabs, Hack-in-the-streets, Hackmeetings

- **¿Qué es un hacklab?**

"Para mí tanto los hackmeetings como los hacklabs representan una interesantísima y fructífera tensión-interacción entre lo social, lo tecnológico y lo político y nacieron con la idea de integrar y contaminar mutuamente a gente de estos campos y aprovechar las sinergias específicas de cada uno guardando un equilibrio inestable necesario para hacer surgir lo mejor de cada uno. En el interno interrogante de quienes somos y hacia donde vamos esta tensión se manifiesta de forma constante y nos obliga a estar repensando y revisando continuamente nuestras posiciones."

AZALAI

- **¿Laboratorio de Hackers?**
- **Social + Tecnológico + Político -> Sinergia**

Hacklabs

- **Nacen en Italia, dentro de Centros Sociales Okupados.**
- **Coincidiendo con la celebración del primer "Hackmeeting" surge el hacklab de Barcelona, Kernel Panic.**
- **Rápidamente el fenómeno se extiende:**
 - **Wau Holland Cielito Lindo Hacklab (Madrid)**
 - **KasLab (Vallecas)**
 - **Metabolik BioHacklab (Leioa)**
 - **La Cuca Albina (Alacant)**
 - **Downgrade (Zrgz)**
 - **Kakelbont (Vitoria-Gasteiz)**
 - **Tenes777 (Parets del Valles, Barcelona)**

Hacklabs



Hacklabs



Hacklabs



Hack in the streets

- **Surgen con la misma idea que los "Reclaim the streets":**
 - **La idea es retomar la calle como un espacio político tecnológico.**
 - **¿Por qué?, porque precisamente la tecnología es lo que está estructurando políticamente nuestra sociedad, tanto en los medios de comunicación, como en la vida cotidiana de la gente.**
 - **Acercar la tecnología a la gente de la calle.**
 - **Demostrar que no es tan inaccesible como pudiera parecer.**

Hack in the streets



Hack in the streets



Hackmeetings

- **No sólo es un encuentro de hackers.**
- **Ni tampoco es tan sólo un encuentro de gente interesada en las nuevas tecnologías y en sus aspectos sociales.**
- **Es un encuentro de gente interesada en las nuevas tecnologías y en sus aspectos sociales que se realiza normalmente en un espacio liberado o CSOA.**
- **Varias ediciones:**
 - **2000: Barcelona, Les Naus.**
 - **2001: Leioa, Udondo Gaztetxea.**
 - **2002: Madrid, Labo03.**
 - **2003: Pamplona, Iruña Gaztetxea.**

Hackmeetings

hAcK yoUr MiNd



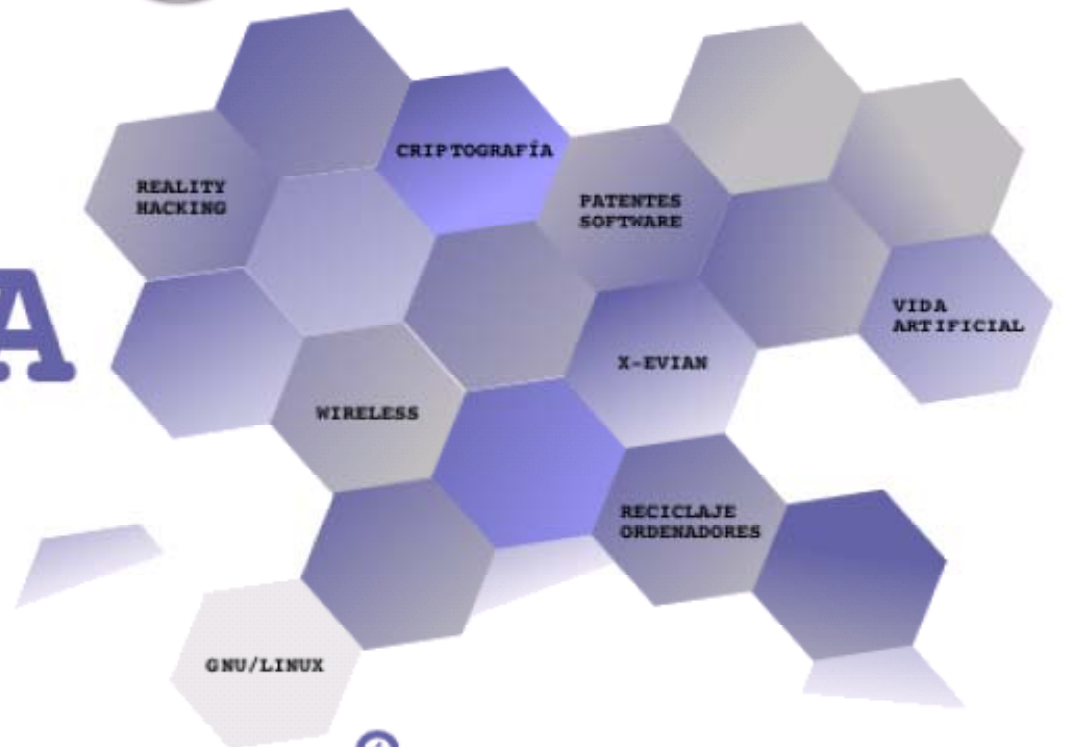
oKupA tU MeNte

HACK3ÑA

IRU

Hackmeeting 2003 Iruña

24, 25, 26 Octubre



Conclusiones

- **Internet y la tecnología han cobrado una importancia muy determinante en nuestras vidas y las del conjunto de la sociedad.**
- **Obviar o desconocer su funcionamiento es dejar las riendas de nuestro futuro en manos de las empresas y gobiernos que más fuerte están pujando por su control.**
- **Existen campañas, grupos e iniciativas que se oponen a ese control y abogan por una tecnología diferente.**
- **Otra tecnología es posible, de hecho, ya está ocurriendo...**